PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

(Chapter II of the Patent Cooperation Treaty)

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference P100566	FOR FURTHER ACTION	See Form PCT/IPEA/416
International application No. **PCT/SG2004/000320**	International filing date *(day/month/year)* 1 October 2004	Priority date *(day/month/year)* 3 October 2003
International Patent Classification (IPC) or national classification and IPC **Int. Cl.** ^{7} H04L 9/14		
Applicant AGENCY FOR SCIENCE, TECHNOLOGY AND RESEARCH et al		

1. This report is the international preliminary examination report, established by this International Preliminary Examining Authority under Article 35 and transmitted to the applicant according to Article 36.
2. This REPORT consists of a total of 3 sheets, including this cover sheet.
3. This report is also accompanied by ANNEXES, comprising:

   a. ☒ *(sent to the applicant and to the International Bureau)* a total of 7 sheets, as follows:

   ☒ sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications authorized by this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions).

   ☐ sheets which supersede earlier sheets, but which this Authority considers contain an amendment that goes beyond the disclosure in the international application as filed, as indicated in item 4 of Box No. I and the Supplemental Box.

   b. ☐ *(sent to the International Bureau only)* a total of (indicate type and number of electronic carrier(s)) , containing a sequence listing and/or table related thereto, in computer readable form only, as indicated in the Supplemental Box Relating to Sequence Listing (see Section 802 of the Administrative Instructions).

4. This report contains indications relating to the following items:

☒	Box No. I	Basis of the report
☐	Box No. II	Priority
☐	Box No. III	Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
☐	Box No. IV	Lack of unity of invention
☒	Box No. V	Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
☐	Box No. VI	Certain documents cited
☐	Box No. VII	Certain defects in the international application
☐	Box No. VIII	Certain observations on the international application

Date of submission of the demand 27 July 2005	Date of completion of the report 10 August 2005
Name and mailing address of the IPEA/AU AUSTRALIAN PATENT OFFICE PO BOX 200, WODEN ACT 2606, AUSTRALIA E-mail address: pct@ipaustralia.gov.au Facsimile No. (02) 6285 3929	Authorized Officer **SUSHIL AGGARWAL** Telephone No. (02) 6283 2192

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/SG2004/000320

Box No. I Basis of the report

1. With regard to the **language,** this report is based on the international application in the language in which it was filed, unless otherwise indicated under this item.

   □ This report is based on translations from the original language into the following language ,
   which is the language of a translation furnished for the purposes of:

   □ international search (under Rules 12.3 and 23.1 (b))

   □ publication of the international application (under Rule 12.4)

   □ international preliminary examination (under Rules 55.2 and/or 55.3)

2. With regard to the **elements** of the international application, this report is based on (*replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report*):

   □ the international application as originally filed/furnished

   ☒ the description:

   pages **1-24** as originally filed/furnished
   pages* received by this Authority on with the letter of
   pages* received by this Authority on with the letter of

   ☒ the claims:

   pages as originally filed/furnished
   pages* as amended (together with any statement) under Article 19
   pages* **25-31** received by this Authority on **8 August 2005** with the letter of **2 August 2005**
   pages* received by this Authority on with the letter of

   ☒ the drawings:

   pages **1-4** as originally filed/furnished
   pages* received by this Authority on with the letter of
   pages* received by this Authority on with the letter of

   □ a sequence listing and/or any related table(s) - see Supplemental Box Relating to Sequence Listing.

3. □ The amendments have resulted in the cancellation of:

   □ the description, pages
   □ the claims, Nos.
   □ the drawings, sheets/figs
   □ the sequence listing (*specify*):
   □ any table(s) related to the sequence listing (*specify*):

4. □ This report has been established as if (some of) the amendments annexed to this report and listed below had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

   □ the description, pages
   □ the claims, Nos.
   □ the drawings, sheets/figs
   □ the sequence listing (*specify*):
   □ any table(s) related to the sequence listing (*specify*):

* *If item 4 applies, some or all of those sheets may be marked "superseded."*

INTERNATIONAL PRELIMINARY REPORT ON PATENTABILITY

International application No.
PCT/SG2004/000320

Box No. V Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Claims **1-17**	**YES**
	Claims **None**	**NO**
Inventive step (IS)	Claims **1-17**	**YES**
	Claims **None**	**NO**
Industrial applicability (IA)	Claims **1-17**	**YES**
	Claims **None**	**NO**

2. Citations and explanations (Rule 70.7)

Following documents were cited in the International Search Report:

D1: WO 2000/049768 A1 (MITTELHOLZER) 24 August 2000

D2: US 2002/0076042 A1 (SANDHU et al.) 20 June 2002

D3: US 5905799 A (GANESAN) 18 May 1999

None of the above prior art documents discloses a method of cryptographically processing a message including determining refreshed decomposition at selected times and after or before the message is processed as specified in claims 1-17.

The claims meet the criteria set out in PCT Articles 33(2-4).

Claims

1. Method for cryptographically processing a message, wherein - a first partial cryptographic key and a second partial cryptographic key, which correspond to a decomposition of a private cryptographic key, are used;
- the message is processed using the first partial cryptographic key resulting in a first partially processed message;
- the message is processed using the second partial cryptographic key resulting in a second partially processed message;
- the first partially processed message and the second partially processed message are combined resulting in a cryptographically processed message,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined and wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

2. The method according to claim 1, wherein the processing of the message using the first partial cryptographic key is carried out by a first computer and the processing of the message using the second partial cryptographic key is carried out by a second computer.

3. The method according to claim 2, wherein the first and the second computer are coupled via a computer network.

4. The method according to claim 2 or claim 3, wherein the method further comprises the step of transmitting the message from the first computer to the second computer.

5. The method according to any of the claims 1 to 4, wherein the first partial cryptographic key and the second partial cryptographic key correspond to a decomposition of the private cryptographic key into a plurality of partial cryptographic keys.

6. The method according to claim 5, wherein the plurality of partial cryptographic keys give, when summed, the private cryptographic key.

7. The method according to any of the claims 1 to 6, wherein the cryptographical processing of the message is the signing of the message or the decrypting of a message.

8. The method according to any of the claims 1 to 7, wherein the message is processed according to a public key cryptographic algorithm.

9. The method according to claim 8, wherein the public key cryptographic algorithm is the RSA algorithm.

10. Computer system comprising
- a first processing unit which is adapted to process a message using a first partial cryptographic key, which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- a second processing unit which is adapted to process a message using a second partial cryptographic key, which

corresponds to the decomposition of the private cryptographic key, resulting in a second partially processed message;

- a combining unit which is adapted to combine the first partially processed message and the second partially processed message resulting in a cryptographically processed message,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

11. Method for generating a cryptographically processed message wherein

- a message is processed using a first partial cryptographic key, which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- the message is transmitted to a client computer;
- a second partially processed message is received which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key;
- the first partially processed message and the second partially processed message are combined to a cryptographically processed message,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

12. Server computer comprising
- a processing unit which is adapted to process a message using a first partial cryptographic key, which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- a transmitting unit which is adapted to send the message to a client computer;
- a receiving unit which is adapted to receive a second partially processed message which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key;
- a combining unit which is adapted to combine the first partially processed message and the second partially processed message to a cryptographically processed message, wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

13. Method for performing a cryptographic operation on a message, wherein
- a message is received;
- the message is processed using a partial cryptographic key which corresponds to a decomposition of a private

cryptographic key resulting in a partially processed message;

- the partially processed message is transmitted to a server computer,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined.

14. Client computer comprising

- a receiving unit which is adapted to receive a message;
- a processing unit which is adapted to process the message using a partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a partially processed message;
- a transmitting unit which is adapted to transmit the partially processed message to a server computer,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined.

15. Computer program element which, when executed by a computer, makes the computer perform the following steps

- processing a message using a first partial cryptographic key which corresponds to a decomposition of a private cryptographic key, resulting in a first partially processed message;
- processing the message using the second partial cryptographic key which corresponds to the decomposition of the private cryptographic key resulting in a second partially processed message;

- combining the first partially processed message and the second partially processed message resulting in a cryptographically processed message,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

16. Computer program element which, when executed by a computer, makes the computer perform the following steps

- processing a message using a first partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a first partially processed message;
- transmitting the message to a client computer;
- receiving a second partially processed message which is the message processed using a second partial cryptographic key which corresponds to the decomposition of the private cryptographic key;
- combining the first partially processed message and the second partially processed message to a cryptographically processed message,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined, wherein the refreshed decomposition is determined by decomposing the first partial cryptographic key and the second partial cryptographic key and combining these decompositions to form a decomposition of the private cryptographic key.

[illegible]
Received 8 August 201

17. Computer program element which, when executed by a computer, makes the computer perform the following steps

- receiving a message;
- processing the message using a partial cryptographic key which corresponds to a decomposition of a private cryptographic key resulting in a partially processed message;
- transmitting the partially processed message to a server computer,

wherein further at selected times and after or before the message is processed, a refreshed decomposition is determined.